IM-SecureSignOn
Version 7.2

セットアップガイド

2012/02/29　初版

＜＜　変更履歴　＞＞

変更年月日	変更内容
2012/02/15	初版

<< 目次 >>

1 はじめに

本ドキュメントは、IM-SecureSignOn のインストール手順と設定の方法について記述しています。
IM-SecureSignOn の標準機能をインストールするには、大きく分けて 2 つの作業が必要です。

1. Login Server モジュールのインストールと設定
2. Web ラッパーモジュールのインストールと設定

■ 用語解説

IM-SecureSignOn	以下、IM-SSO と略します。
intra-mart WebPlatform	以下、IWP と略します。
intra-mart AppFramework	以下、AFW と略します。

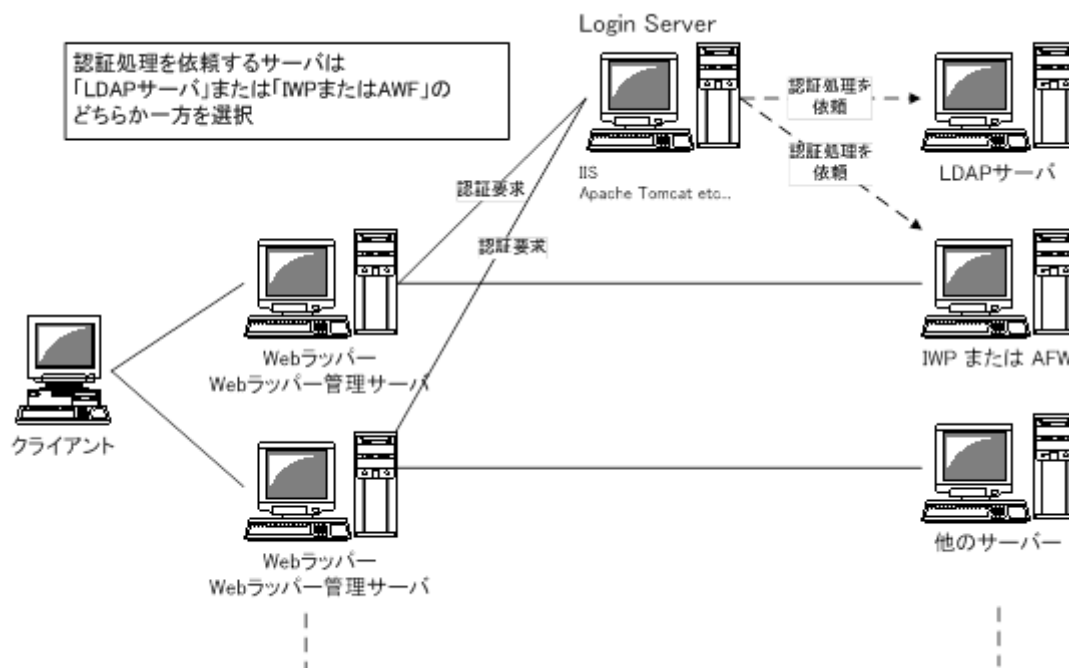
その他の拡張モジュールのインストールは、各ディレクトリの doc 以下のドキュメントを参照してください。

2 前提条件

IM-SecureSignOn Ver7.2 をインストールするためには、以下の前提条件があります。

■ IWP Ver.7.2 または AFW Ver.7.2 が正常に動作していること。
IWP または AFW のパッチに関しましては、常に最新のものを適用するようにしてください。

3 インストール手順

3.1 システム構成

3.2 インストールファイル構成

sso	IM-SSO ディレクトリ
├ basic-proxy	Basic 認証保存プロキシモジュールディレクトリ
├ LoginServer	Login Server モジュールディレクトリ
├ mobile	モバイルゲートウェイモジュールディレクトリ
├ sso-repository	SSO リポジトリモジュールディレクトリ
├ tool	ツール格納ディレクトリ
├ wrapper	Web ラッパーモジュールディレクトリ
├ wrapper-plugin	Web ラッパーJavaScript プラグインモジュールディレクトリ
├ setup_guide_v72.pdf	セットアップガイド
└ release_notes_v72.pdf	リリースノート

3.3 Login Server の環境設定

以下の手順で、Login Server の環境設定を行います。

環境設定の詳細については、以下の章で順に説明しています。

1. セキュリティプロバイダの追加
2. war ファイルの展開
3. 鍵セットの作成
4. 設定ファイルの編集
5. デプロイ

※ より詳しい説明については、

sso/LoginServer/doc/SSO ログインサーバ V320-取扱説明書.pdf

を参照してください。

3.3.1 セキュリティプロバイダの追加

下記の作業手順に従って、セキュリティプロバイダの追加を行います。

※ 以下、JDK のインストールディレクトリを $JAVA_HOME として説明します。

1. 暗号プロバイダの追加
   Bouncy Castle 暗号プロバイダをインストールします。
   http://www.bouncycastle.org/latest_releases.htmlより配布されているJCEプロバイダ
   (bcprov-jdkXX-YYY.jar)を
   $JAVA_HOME/jre/lib/ext/ ディレクトリに配置してください。
   ※ 使用するJREに合わせたバージョン(XXの数字が 15 または 16)を用います。

2. java.security へ暗号プロバイダの追加
   $JAVA_HOME/jre/lib/security にある java.security ファイルをテキストエディタで開き、
   セキュリティプロバイダ一覧に、 Bouncy Castle 暗号プロバイダを追加します。

   security.provider.n で始まる行の次に、以下の設定例を参考に追加してください。

■ 設定例（JDK 1.6.0_30 の場合）

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
security.provider.7=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.8=sun.security.smartcardio.SunPCSC
security.provider.9=sun.security.mscapi.SunMSCAPI
security.provider.10=org.bouncycastle.jce.provider.BouncyCastleProvider
```

3.3.2 war ファイルの展開

設定ファイルや鍵セットファイルを更新するために、war ファイルを展開します。
(sso/LoginServer/bin/sso.war)
war ファイルの展開には、J2EE に付属の jar コマンドを使用するか、ZIP 形式の圧縮ファイルを展開することが可能なツールを使用してください。

※ 以下、sso.war ファイルを展開したディレクトリを、<%sso_path%> として説明します。

jar コマンドによる、war ファイルの展開例

```
c:¥sso> jar xf sso.war
```

3.3.3 鍵セットの作成

付属の「SSO 鍵ファイル作成ツール」（sso/tool/CertMaker/bin/CertMaker.exe）を
使用して、電子署名および暗号化／複合化に使用する鍵セットを作成します。

操作方法の詳細については、「鍵ファイル作成ツール取扱説明書」
sso/tool/CertMaker/doc/鍵ファイル作成ツール説明書.pdf
を参照してください。
※ 鍵ファイル作成ツールは Windows2000 または XP にて使用してください。

作成した鍵セットは、 sso.war ファイルを展開したディレクトリ下の WEB-INF/signature/ ディレクトリに
格納してください。

■ 鍵セットの格納先

鍵セット	ディレクトリ	ファイル名
秘密鍵ファイル	<%sso_path%>/WEB-INF/signature/	key.pem
証明書ファイル	<%sso_path%>/WEB-INF/signature/	cert.pem

※ 既存のファイルがある場合は、上書きして構いません。

3.3.4　設定ファイルの編集

■ イントラマートでの設定

※ 以下、イントラマートをインストールしたディレクトリを、<%im_path%> として説明します。
イントラマートの <%im_path%>/conf/access-security.xml ファイルをエディタで開き、
access-security/security-config/user-security/initial-request-analyzer タグに以下の項目を追加します

param-value タグには、intra-mart からログアウトした後に表示されるページ(URL)を指定しています。
標準の設定では、LoginServer のログアウト画面を設定します。
※ Login Server に SSL を適用する場合は、https://・・・ から始まる値を指定してください。

```
<initial-request-analyzer>
    <request-analyzer-class>
        jp.co.intra_mart.foundation.security.certification.SSORequestAnalyzer
    </request-analyzer-class>
    <init-param>
        <param-name>sso-logout-url</param-name>
        <param-value>http://LoginServer のホスト名/sso/logout.do </param-value>
    </init-param>
</initial-request-analyzer>
```

記述例:

```
<access-security>
    :
  <security-config>
        :
    <user-security>
        <initial-request-analyzer>
            <request-analyzer-class>
                jp.co.intra_mart.foundation.security.certification.SSORequestAnalyzer
            </request-analyzer-class>
            <init-param>
                <param-name>sso-logout-url</param-name>
                <param-value>http://auth.intra-mart.jp/sso/logout.do</param-value>
            </init-param>
        </initial-request-analyzer>
            :
    </user-security>
    :
  </security-config>
      :
</access-security>
```

(注意)
本マニュアルでは、ホスト名の後のポート番号を **80** 番と想定し省略してあります。
実際の利用の際には、各ホストに対応するポート番号を必要に応じて付加してください。

■ Login Server での設定

※ 以下、sso.war ファイルを展開したディレクトリを、**<%sso_path%>** として説明します。

1. Login Server の <%sso_path%>/WEB-INF/sso-login.xml ファイルをエディタで開きます。

2. sso-login.xml の sso-login/authenticate/intra-mart/url タグを以下のように書き換えます。
   <url>**http://<intra-mart サーバ名>:<ポート番号>/imart/CertServlet**</url>

   記述例:

```
<sso-login>
      :
    <authenticate>
          :
        <intra-mart>
            :
            <url>http://imart.intra-mart.jp:8080/imart/CertServlet</url>
        </intra-mart>
    </authenticate>
      :
</sso-login>
```

3. sso-login.xml の sso-login/domain/ タグ内の name、login-url、logout-url 属性を
   以下のように書き換えます。
   name=”**.Login Server 名を除いたドメイン名”** →（注意）「**.**」から記述すること。
   login-url=”**http:// Login Server のホスト名/sso/login.do**”
   logout-url=”**http:// Login Server のホスト名/sso/logout.do**”

   記述例:

```
<sso-login>
    :
    <domain
        name=".intra-mart.jp"
          :
        login-url="http://auth.intra-mart.jp/sso/login.do"
        logout-url="http://auth.intra-mart.jp/sso/logout.do"
          :
     />
      :
</sso-login>
```

※ Login Server に SSL を適用する場合は、http://･･･と記述している箇所を https://･･･ から始まる値を指定してください。

4. sso-login.xml の sso-login/environment/portal_url タグを編集することで、
   ログインのキャンセル時や、LoginServer のログアウト画面のボタン押下時に遷移先が指定されていない場合のデフォルトの遷移先 URL を指定します。

   標準の設定では、Web ラッパーの URL を指定します。
   http:// Web ラッパーのホスト名 / ACL 設定のパス / ログイングループ.portal

■ 記述例: ログイングループが **default** の場合

```
<sso-login>
    :
  <environment>
      :
      <portal_url>http://web.intra-mart.jp/imart/default.portal</portal_url>
  </environment>
    :
</sso-login>
```

3.3.5 認証エラー時のメッセージ設定について

intra-mart 側での認証エラーに対するメッセージを設定することができます。
標準の実装では、ログイングループが存在しない場合とシステムエラー時にはその旨を知らせる独自のメッセージを表示するよう設定されています。

■ 既存エラーメッセージ表示設定
標準の実装では、アカウントロック/ライセンス無効/ユーザが存在しない
これらの場合について、通常のログイン失敗時のエラーメッセージを表示するよう設定されています。
それぞれのエラー内容を通知するメッセージを表示させるようにするには、sso-login.xml 内の message-mapping タグのコメントアウトを外します。
また、エラーメッセージをデフォルトのものにしたい場合は該当する message-mapping タグをコメントアウトします。

例:ライセンス無効のエラー情報を表示させる場合、
<message-mapping id="-1" property="im.login.no.license"/>
をコメントアウトから外す。
例:ログイングループが存在しない場合のエラーメッセージを標準のものにする
<message-mapping id=”-2” property=”im.login.no.group”/>
をコメントアウトする。

■ 既存エラーに対するメッセージの編集
標準のエラーメッセージを変更するためには、MessageResources_ja.properties を編集します。
プロパティファイルはマルチバイト文字が UTF-8 エンコード("¥u"+16 進数)されているため、設定内容を変更する場合は、以下の手順で実施してください。

1. 同一ディレクトリにある MessageResources_ja.properties.SJIS ファイルを編集します。
   このファイルはマルチバイト文字がシフト JIS で記述されています。

2. Java に付属する native2ascii コマンドで、UTF-8 エンコードしたファイルを作成します。

   native2ascii –encoding Windows-31J
   MessageResources_ja.properties.SJIS MessageResources_ja.properties
   (実際には一行で実行してください)

3.3.6 認証を行うログイングループの解決方法について

標準の実装では認証を行う時、最初に入力された URL から認証対象となるログイングループを決定しています。たとえば **http://web.intra-mart.jp/imart/default.portal** でアクセスした場合、**default.portal** のピリオドの前の文字列、default が認証対象のログイングループとなります。
認証処理は認証対象のログイングループ内のユーザで行われます。

認証対象のログイングループを固定的に設定したい場合は、以下のようにパラメータを追加します。
この設定を行うことで、認証は必ず指定したログイングループ内のユーザで認証されます。
<login-group-name>ログイングループ</login-group-name>

記述例:

```
<sso-login>
    :
    <authenticate>
        :
        <intra-mart>
            :
            <login-group-name>default</login-group-name>
        </intra-mart>
    </authenticate>
    :
</sso-login>
```

3.3.7 デプロイ

1. 変更内容を反映した war ファイルを作成します。
   war ファイルの作成には、J2EE に付属した jar コマンドを使用してください。
   - jar コマンドによる、war ファイルの作成例

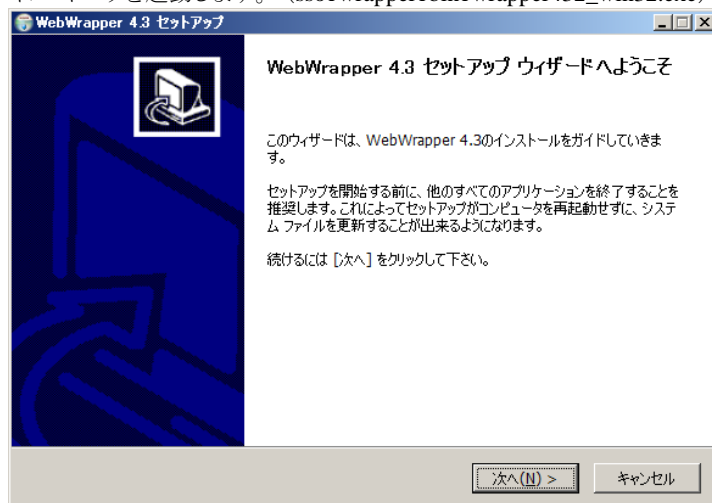
   ```
   c:¥sso> jar cf sso.war *
   ```

2. J2EE サーバへデプロイします。
   コンテキストルートパスは sso に設定してください。
   ※ J2EE サーバへのデプロイ方法については、使用されるパッケージのマニュアルをご覧ください。

（注意）
ほとんどの J2EE サーバは、Web アプリケーションの位置をディレクトリで指定することが可能です。
この場合は、war ファイル化せずに、war ファイルを展開したディレクトリの親ディレクトリを指定してください。

3.4 Web ラッパーのインストール

3.4.1 Windows 版のインストール

インストーラを起動します。（sso¥wrapper¥bin¥wrapper432_win32.exe）

ウィザードに表示される以下の質問に回答しながら、インストールを進めてください。

1. インストール先フォルダの選択
   インストール先のフォルダを入力、または［参照］ボタンより選択して、[次へ]ボタンを押下してください。
   （例）C:¥Program Files¥SSO
2. Web ラッパー管理ツールの情報を設定
   以下の記述例を参考に、各項目の情報を設定してください。

項目	記述例	説明
サービス名	imsso	任意の名前を設定。 ※1 台の Web サーバに複数の Web ラッパーをインストールする際に、区別するための名称です。
ポート番号	8090	Web ラッパー管理ツールが常駐するポート番号を設定。 ※他で使用されていないポート番号を指定してください。
接続許可する IP アドレス	192.168.0.1	Web ラッパー管理ツールに接続を許可する端末名、 または IP アドレス、ネットワークアドレスを設定します。
アカウント	sysuser	システム設定アカウントを設定。
パスワード	acluser	システム管理者アカウントのパスワードを設定。

※接続許可する IP アドレスには、複数指定することが可能です。その場合は、カンマ区切りで設定します。

例 ：

```
localhost,mypc,192.168.0.1
```

ローカルホスト、mypc という名前の端末、192.168.0.1 の IP アドレスを持つ端末から、
接続を許可する設定となります。

3. ［インストール］ボタンを押すと、インストールが開始します。
4. インストールが終了したら、[完了］ボタンを押してウィザードを閉じてください。
   以上で Web ラッパーのインストールは完了です。

3.4.2 Solaris/Linux 版のインストール

1. 配布アーカイブファイルの展開

展開するアーカイブファイルは、 sso/wrapper/bin ディレクトリ内にあります。

以下のコマンド例により、インストール先のディレクトリにファイルを展開してください。

```
% gunzip -c wrapperd_xxx.tar.gz | tar xvf -
```

SSO ディレクトリが作成され、ファイルが展開されます。

※ コマンド例で示した、ファイル名の「xxx」の部分は、各プラットフォームよって異なります。

ご利用の環境にあわせて変更してください。

（注意）

既に存在するファイルは上書きされてしまいますので、バージョンアップインストールの場合は、
事前に設定ファイル等を退避させてください。

2. ファイルオーナー、パーミッションの変更

Web ラッパー管理ツールから Web ラッパーの「起動／停止」が行えるように設定します。
以下のコマンドを実行してください。

```
# chown root SSO/wrapperd/wrapperd
# chmod 755 SSO/wrapperd/wrapperd
```

3. ディレクトリオーナーの変更

Web ラッパーは通常 nobody で実行されます。インストール先ディレクトリの所有者を nobody に変更します。適切な所有者が設定されないと、ログファイルを書き込めないため、Web ラッパーは起動に失敗します。
以下のコマンドを実行してください。

```
# chown nobody:nobody SSO/wrapperd/
```

4. Web ラッパー管理ツールの設定

付属のツールを使用して、Web ラッパー管理ツールの設定を行います。

```
% SSO/wrapadmin/makeconf
```

（注意）

SSO/wrapadmin/makeconf 及び SSO/rc/wrapperd ファイルについて、必要に応じてファイル内にある
INSTDIR= 以降に Web ラッパーをインストールしたディレクトリを指定してください。
（デフォルトでは/opt/SSO）

次の質問に対して、適切な値を設定してください。

i) Webラッパー管理ツールが使用するポート番号

ii) システム設定アカウント

iii) システム設定アカウントのパスワード

iv) Web ラッパー管理ツールへのアクセス可能端末名

名前解決が可能なホスト名、IP アドレス、ネットワークアドレスによる指定が可能です。

例： localhost,mypc,192.168.0.1

（ローカルホスト、mypc という名前の端末、192.168.0.1 の IP アドレスを持つ端末から、
接続を許可します。）

3.5 intra-mart ユーザ認証モジュールの設定

3.5.1 基本設定

Web ラッパー管理ツールで設定を行います。

1. ブラウザから Web ラッパーの管理ツールを起動します。管理者でログインしてください。

［管理者］ユーザ名　：Web ラッパーのインストール時に設定したアカウント

パスワード　：Web ラッパーのインストール時に設定したパスワード

2. 左ページメニューから [システム設定]-[基本設定] をクリックします。

3. 右画面の各フィールドが、以下の設定になっていることを確認してください。
以下の内容を「例」として、各項目の設定について説明します。
※ 実際に設定を行うときは、ご利用の環境に合わせて値を変更してください。

Web ラッパー　：web.intra-mart.jp

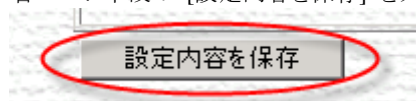
Login Server　：auth.intra-mart.jp

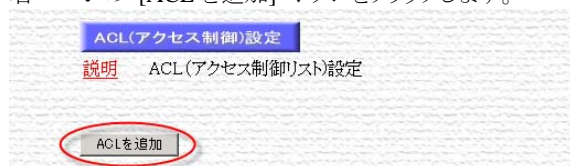
IWP/AFW　：imart.intra-mart.jp

■ 全体的な設定

項目	設定内容
RemoteName	IWP/AFW のホスト名（ドメイン名またはIPアドレス） 例 ： imart.intra-mart.jp
RemotePort	IWP/AFW のポート番号
HostName	Web ラッパーのホスト名（このサーバのホスト名です。） 例 ： web.intra-mart.jp
LocalPort	Web ラッパーのポート番号 （注意）Web ラッパー管理ツールのポート番号ではありません
User	Web ラッパー起動ユーザ**(Solaris/linux 専用メニュー)**
Group	Web ラッパー起動グループ**(Solaris/linux 専用メニュー)**
AuthURL	Login Server URL(ログイン認証) のURL 例 ： http://auth.intra-mart.jp/sso/login.do
ReAuthURL	Login Server URL(再認証) のURL 例 ： http://auth.intra-mart.jp/sso/login.do
CancelURL	認証キャンセル時の表示 URL（空白）
IpMismatchURL	CheckIP でアドレス不一致の場合に表示する URL 例 ： http://auth.intra-mart.jp/sso/msg/ipmismatch.jsp
InvalidSignURL	CheckSignature で署名不正の場合の表示 URL 例 ： http://auth.intra-mart.jp/sso/msg/invalidsign.jsp
FormatErrURL	認証データフォーマットエラー時の表示 URL 例 ： http://auth.intra-mart.jp/sso/msg/formaterr.jsp
CookieDomain	要求、応答クッキーの送出ドメイン（サーバ名を除いたドメイン名） 例 ： .intra-mart.jp（‘.’から始まります）
CertFile	認証クッキー電子署名検証用証明書 cert.pem ファイルの内容を設定

※ **Login Server** に **SSL** を適用する場合は、**http** と記述する箇所を **https://**･･･から始まる値を指定してください。

4. 右ページ下段の [設定内容を保存] をクリックします。

5. 左ページのメニューから [ACL 設定] をクリックします。

6. 右ページの [ACL を追加] ボタンをクリックします。

7. 以下のように入力し、[設定内容を保存]ボタンをクリックします。

ACL(アクセス制御)設定
説明　ACL(アクセス制御リスト)設定
コメント：
パス：/imart/
アクセス条件：(comid=*)
有効期限：
アクセス権なし時の表示ファイル名
許可IPアドレス：
拒否時送出ファイル名
拒否IPアドレス：
このアクセス制御を削除
ACLを追加
設定内容を保存

（補足）

intra-mart を認証する場合は、以下に示す情報を得ることができます。

必要に応じて、アクセス条件に項目を追加して、アクセス制御を行ってください。

項目	内容
comid	ユーザ情報（ユーザ ID とログイングループの ”/” 区切り → uid/lgngrp） （例）master/DEFAULT ※ただし、ログイングループが未指定の場合は、ユーザ ID のみ
uid	ユーザ ID
lgngrp	ログイングループ
pwd	パスワード
name	ユーザ名
madrs	メールアドレス
mbladrs	モバイルメールアドレス
roles	ロール名一覧（ロール名の ”|” 区切り） （例）|super|guest|user1|user2|

アクセス条件の記述方法について、いくつかの例を以下に示します。 参考にしてください。

■ 複数のアクセス条件を指定する場合は、「&」 でつなげる

（例）

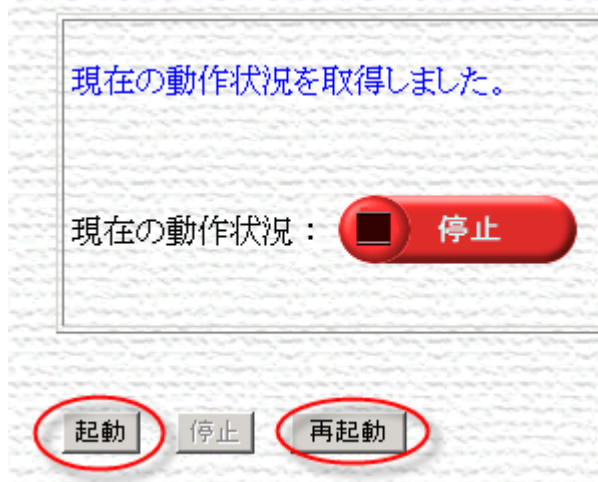
```
(comid=*)&(uid=*)&(roles=*)
```

■ 「管理者ロール（super）」 を条件に指定する場合

（例）

```
(roles=*|super|*)
```

1. 左ページのメニューから [起動／停止] をクリックします。

2. 右ページの [起動] または[再起動] ボタンをクリックして、起動します。

以上で、Web ラッパー管理ツールでの設定は終了です。

3.5.2 形式変換プラグインの設定

Login Server で使用する Apache Tomcat において 5.5.26 以降または 6.0.16 以降のバージョンを使用する場合には、「形式変換プラグイン」の設定を行う必要があります。設定方法は以下の通りです。

詳細については、
「VANADIS SSO WebWrapper 4.1/4.2/4.3/4.4 形式変換プラグイン 1.0.0【インストール・設定マニュアル】」
sso/ wrapper-plugin/quotedcookie/doc/形式変換プラグイン_インストール・設定マニュアル.pdf
を参照してください。

■ プラグインファイルの配置

※ 各 OS のプラグラインファイルは、sso/ wrapper-plugin/quotedcookie/bin 配下の各 OS 名のディレクトリに保存されています。

1. Windows 版

Web ラッパーの実行モジュール(wrapperd.exe) があるディレクトリ
(例:C:¥ProgramFiles¥SSO¥default¥wrapperd)に
プラグインファイル quotedcookie.dll をコピーします。

2. Solaris/Linux 版

Web ラッパーの実行モジュール(wrapperd または wrapperd.bin) があるディレクトリ
(例:/usr/local/SSO/wrapperd)に
プラグインファイル quotedcookie.so(HP-UX 環境では、拡張子は.so ではなく sl)をコピーします。

また、HP-UX 環境では、本プラグインに実行権限が付与されていなければなりません。必要に応じてコマンド(chmod +x ファイル名)を実行してください。

■ 設定

Web ラッパー管理ツールで設定を行います。

1. プラグインライブラリファイル名の設定

Web ラッパー管理ツールの[システム設定]→[カスタム設定]より、『LoadPlugin』(プラグインライブラリファイル名)にコピーしたプラグインファイル名を入力します。

または、WebWrapper 設定ファイル(server.conf) の GLOBAL セクション "LoadPlugin"ディレクティブにコピーしたプラグインファイル名を記述します。

2. 本プラグイン独自の設定

Web ラッパー設定ファイル(server.conf)へ直接、または、Web ラッパー4.3.1(以降)管理ツールの[上級者設定]→[システム設定]より、下記の内容を追加します。

```
[Format] QuotedCookie enable
```

すべての設定が完了しましたら、Web ラッパーを再起動して設定を反映させます。

4　　動作確認

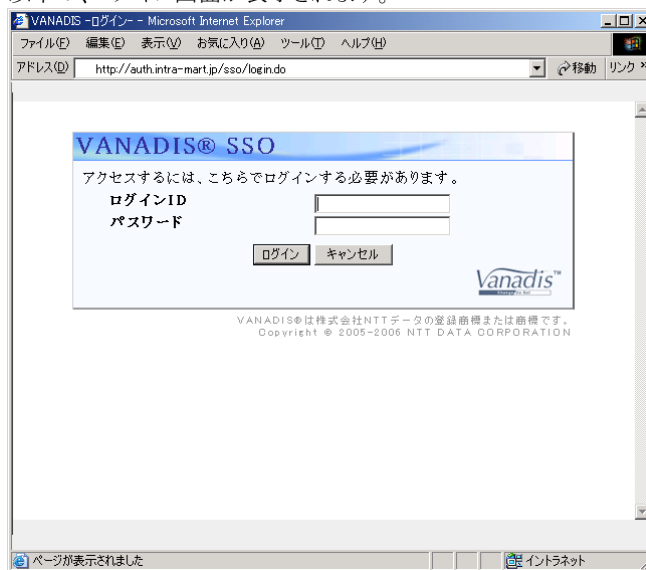
SSO 認証サーバおよび、Web ラッパーが起動していることを前提に、SSO の動作確認を行ってください。

1. ブラウザから、以下のような URL を発行します。
   http:// Web ラッパーのホスト名 / ACL 設定のパス / ログイングループ.portal

   ※ Webラッパーのホスト名には、「3.5.1 基本設定」の 3
   で［HostName］項目に設定したものを記述します。
   ※ ACL設定のパスには、「3.5.1 基本設定」の 7 で設定したものを記述します。

   （例）以下の内容で設定した場合、URL は
   http://web.intra-mart.jp/imart/default.portal　となります。

   Web ラッパーのホスト名　：web.intra-mart.jp
   ACL 設定のパス　：/imart/
   ログイングループ　：default

2. 以下の、ログイン画面が表示されます。

3. 任意のユーザで、イントラマートにログインします。
   イントラマートのメインページが表示されます。

4. イントラマートをログアウトすると、LoginServer のログアウト画面が表示されます。

5. 「OK」ボタンを押下します。
   以下の、ログイン画面が表示表示されたら、インストールおよび設定は成功です。

IM-SecureSignOn Ver.7.2
セットアップガイド

2012/02/29 初版

TEL: 03-5549-2821
FAX: 03-5549-2816
E-MAIL: info@intra-mart.jp
URL: http://www.intra-mart.jp/